D4US LLC dba Dimension4

POLICY AND PROCEDURES GOVERNING CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)

D4US LLC dba Dimension4
382 NE 191st Suite #59205
Miami, FL 33179-3899

Table of Contents

Introduction & Statement of Company Policy

Under applicable federal and state laws, **D4US LLC dba Dimension4** (the "Company") has a duty to protect the confidentiality of proprietary information of, and relating to, customers, other telecommunication carriers, and equipment manufacturers. To ensure full compliance with these laws and regulations, including, specifically, the rules of the Federal Communications Commission governing customer proprietary network information ("CPNI"), this Manual sets forth in detail the policy and procedures of **D4US LLC dba Dimension4** governing the use, disclosure, and provision of access to such proprietary information.

Questions regarding compliance with the policies and procedures set forth in this Manual should be directed to the Company's Chief Financial Officer or D4US dedicated email compliance@myd4.com.

POLICY STATEMENT

Each employee and authorized agent of the Company is required to protect the confidentiality of customer proprietary network information ("CPNI") and, to that end, shall comply with all policies and procedures set forth in this manual.

- Each employee and authorized agent of the Company is required to protect the confidentiality of proprietary information of other telecommunications carriers and equipment manufacturers, and to that end, shall comply with all policies and procedures set forth in this manual.

- Any violation of or departure from the policies and procedures set forth in this manual shall be reported to the Company's Chief Financial Officer.

- Any failure to comply with the policies and procedures set forth in this manual shall result in disciplinary action including, but not limited to, suspension and/or termination of employment

1.0 APPLICABILITY

The policies and procedures set forth in this manual apply to all employees, officers, directors, and authorized agents of **D4US LLC dba Dimension4** (or the "Company).

2.0 DEFINITIONS

2.1 "Customer proprietary network information" means

(a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by the carrier-customer relationship; and

(b) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;
except that such term does not include subscriber list information.

2.2 *Account information*. "Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, contracted services or the bill's amount.

2.3 *Address of record.* An "address of record" whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

2.4 *Call detail information*. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

2.5 *Readily available biographical information.* "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

2.6 *Telephone number of record.* The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

3.0 GENERAL DUTY OF THE COMPANY

The Company, including all employees, officers, directors, and authorized agents of the Company, have a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

4.0 CONFIDENTIALITY OF CARRIER INFORMATION

The Company may use proprietary information received or obtained from another telecommunications carrier for the purpose of providing any telecommunications service only for that purpose.

5.0 CONFIDENTIALITY OF CPNI

5.1 Privacy Requirements - Generally. The Company may only use, disclose, or permit access to individually identifiable CPNI –

(a) as **required by law**;

(b) with the **approval of the customer**; or

(c) **in providing the telecommunication service from which the CPNI is derived** or in providing services necessary to, or used in, providing such telecommunications service.

5.2 Disclosure upon Request by Customers. The Company shall disclose CPNI, upon affirmative written request by the customer, to any person designated by the customer.

6.0 CONDUCT EXPRESSLY PROHIBITED BY THE COMPANY

6.1 The following are expressly prohibited by the Company:

(a) Sale or possession of CPNI.

The Company prohibits the sale and/or possession of CPNI, and any other conduct undertaken for a fee for the purpose of using, disclosing, or permitting access to CPNI in violation. The Company prohibits any attempt

to sell, obtain possession of, or otherwise acquire or arrange for unauthorized access to CPNI, including any effort to induce another to permit an unauthorized use, disclosure or access to CPNI.

(c) Use of CPNI to track customers' use of competitors' services.

The Company prohibits the use, disclosure or provision of access to CPNI to identify or track customers that call competing service providers.

6.2 Any violation of this section shall be grounds for immediate termination of employment and, as applicable, referral to federal and/or state law enforcement authorities for further action. The Company may, however, in its discretion take alternative disciplinary action against any employee, officer, director or authorized agent of the Company found to have violated this section.

7.0 PERMITTED USES AND DISCLOSURES OF CPNI

The Company may use CPNI obtained from its customers, either directly or indirectly through its agents --

7.1 To initiate, render, bill and collect for telecommunications services;

7.2 To provide marketing, in compliance with FCC rules;

7.3 To protect the rights or property of the Company, or to protect users and other carriers from fraudulent or illegal use of, or subscription to, such services;

7.4 To provide call location information concerning the user of a commercial mobile service in the following emergency situations:

(a) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(b) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(c) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency;

7.5 For the provision of information services;

7.6 In its provision of maintenance and repair services.

8.0 COMPANY POLICIES & PROCEDURES

8.1 Unauthorized Use of CPNI.

The Company regards any unauthorized or improper use, disclosure or access to CPNI as a serious offense, and will take appropriate disciplinary action, which may include suspension and/or termination of employment. In addition:

(a) The Company may require any employee, officer or director found to have made unauthorized or improper use of CPNI to undergo training to ensure future compliance.

8.2 CPNI Requested by Law.

An employee who receives a request to provide CPNI pursuant to legal process, such as a subpoena or warrant, shall provide such information only after verification of the identity of the requesting agency or officer.

8.3 Customer Requests for CPNI.

(a) CPNI may be disclosed only to the customer or a third party designated by the customer to receive the customer's CPNI. The Company requires all employees to ensure that the person requesting CPNI is authorized to receive such CPNI. The company requires authentication of a customer's identification prior to the release of CPNI on customer initiated telephone contacts, online account access, and email requests. Customer interaction that requires CPNI authentication includes any, but is not limited, to the following:

Adds, Moves and Changes

- Password resets
- Account information
- VM access and resets
- Telephone number changes such as call forwarding
- Email access or changes

Access to on site equipment

- Username and passwords for onsite equipment

(b) **Email request from unauthorize pre-stablished users:** The Company does not accept customer requests for CPNI via email, unless (a) CPNI pre-stablished password is provided on the originating email (b) one of the secret questions answer is provided.

(c) **Email request from authorized users:** The company will accept customer request for CPNI via email if the request comes from authorized point of contact(s) that have been pre-stablished via the "customer action required letter" or as reflected in our Company systems.

(d) **Customer initiated call:** The Company will disclose CPNI information, including call detail, on a customer initiated call only if the customer provides a pre-established password or one of the secret questions answer is provided. If no password has been established or if the customer does not provide any of the requirements above the company will not release the information except by sending them to an address of record, calling the customer at the telephone of record, or emailing the authorized point of contacts in our system.

(e) **Unauthorized users for customer initiated call:** If the caller is able to provide call detail information to the Company's employee during a customer-initiated call without the Company employee's assistance, then the employee is permitted to discuss the call detail information provided by the customer. If the unauthorized user can provide the CPNI password, or respond any of the secret questions, information and assistance can be provided.

(f) **Contacts to customer support:** Agent must verify the following when a customer calls in asking to make changes or get information on account

1. CPNI password: you may find this in CRM
2. Answers one of the two secret questions.
3. Person calling is in the contact list

If the person does not know the CPNI password we will not be able to assist until they either get the code or an authorized contact at the company calls/emails approving the changes or giving us permission to work with the person.

(g) The Company allows CPNI to be disclosed to a third party designated by the customer to receive his or her CPNI only pursuant to written authorization from the customer. The following is required for a written authorization to be valid: the customer's full name, street address, social security number, date of birth, and the telephone number(s) for which CPNI is requested. The authorization must be signed by the person whose name appears on the account as the customer of record. The Company will accept only a signed original authorization.

8.4 Online account Access.

The Company requires the authenticated password or the answer to one of the secret questions to access CPNI on-line. If a customer cannot provide any of the above the company will authenticate the customer based upon the methods listed in 8.3 (c).

8.5 Notice to Customers of Account Change.

The Company will notify the customer immediately when the following are created or changed by Dimension4 representatives: (1) a password; (2) a back-up for forgotten passwords; (3) an online account; (4) the address of record. This notification may be through a Company originated voicemail or call to the telephone number of record, or by email to authorized point of contacts, as to reasonably ensure that the customer receives the notification. If unable to reach the customers thru those means, a formal mail letter will be sent to the address of record with the changes.

8.6 Records of Disclosure of CPNI.

The Company shall maintain a record of its own or any affiliates sales and marketing campaigns (if any) that use their customers' CPNI. The Company's Vice President of Sales & Marketing is responsible for maintaining this record, which shall include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. This record shall be kept for a minimum of one year.

8.7 Duty to Report Violation or Departure from CPNI Policies and Procedures Manual

Each employee, officer, director and authorized agent of the Company has an affirmative duty to ensure compliance by the Company of the requirements under federal and state law governing the use of CPNI. Any employee, officer, director or authorized agent of the Company who knows of or has reason to believe that a violation of or departure from the policies and procedures set forth in this Manual has occurred or will occur shall immediately notify your immediate Manager/Supervisor, Executive Officers, the CEO, or any member of the Board of Directors if the CEO is the subject of the suspected violation.

8.8 Notice to Law Enforcement of Unauthorized Disclosure of CPNI

(a) The Company must notify law enforcement of a breach of its customer's CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation. The Company will not notify customers or disclose the

breach to the public until 7 full business days have passed after the notification to the USSS and the FBI except as provided in FCC CPNI rules.

(b) The company will maintain a record of any breaches discovered, notifications made to the USSS and the FBI and notifications made to customers. The record will include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach and the circumstances of the breach. The record must be retained for 2 years.

8.9 Employee Annual Certification

All employees of the Company shall be given a copy of this Manual. All employees are required annually to review the manual and to certify in writing that he or she understands and will adhere to the policies and procedures in this manual.

8.10 Annual Certificate of Compliance.

A Company Officer shall annually sign a CPNI compliance certificate stating that the officer has personal knowledge that the Company has established policies and procedures that are adequate to ensure compliance with the FCC's CPNI rules.

RECEIPT AND ACKNOWLEDGMENT

I acknowledge that I have received a copy of the manual on **D4US LLC dba Dimension4** Policies and Procedures Governing Customer Proprietary Network Information ("Manual").

I understand that I am responsible for knowing and adhering to the policies within the Manual. I understand that any infractions of the foregoing policies may constitute grounds for the termination of my status with the company, or other disciplinary measures.

	Anthony Zabit
Company	**D4US LLC dba Dimension4**
Date	**4/5/2018**
Company Officer	**Anthony Zabit**

For questions or doubts about this process contact compliance@myd4.com.